IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICANTS	:	Hak-Phil Lee et al.
SERIAL NO.	:	Not Yet Assigned
FILED	:	January 16, 2004
FOR	:	GIGABIT ETHERNET-BASED PASSIVE OPTICAL NETWORK AND DATA ENCRYPTION METHOD

PETITION FOR GRANT OF PRIORITY UNDER 35 USC 119

MAIL STOP PATENT APPLICATION
COMMISSIONER FOR PATENTS
P.O. BOX 1450
ALEXANDRIA, VA. 22313-1450

Dear Sir:

Applicant hereby petitions for grant of priority of the present Application on the basis of the following prior filed foreign Application:

COUNTRY	SERIAL NO.	FILING DATE
Republic of Korea	2003-59018	August 26, 2003

To perfect Applicant's claim to priority, a certified copy of the above listed prior filed Application is enclosed. Acknowledgment of Applicant's perfection of claim to priority is accordingly requested.

Respectfully submitted,

Steve S. Cha
Attorney for Applicant
Registration No. 44,069

CHA & REITER
210 Route 4 East, #103
Paramus, NJ 07652
(201) 226-9245

Date: January 16, 2004

Certificate of Mailing Under 37 CFR 1.8

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to MAIL STOP PATENT APPLICATION, COMMISSIONER FOR PATENTS, P. O. BOX 1450, ALEXANDRIA, VA. 22313-1450 on January 16, 2004.

Steve S. Cha, Reg. No. 44,069
Name of Registered Rep.)

(Signature and Date) 1/16/04

대 한 민 국 특 허 청
KOREAN INTELLECTUAL PROPERTY OFFICE

별첨 사본은 아래 출원의 원본과 동일함을 증명함.

This is to certify that the following application annexed hereto is a true copy from the records of the Korean Intellectual Property Office.

출 원 번 호 : 10-2003-0059018
Application Number

출 원 년 월 일 : 2003년 08월 26일
Date of Application AUG 26, 2003

출 원 인 : 삼성전자주식회사
Applicant(s) SAMSUNG ELECTRONICS CO., LTD.

2003 년 09 월 25 일

특 허 청
COMMISSIONER

【서지사항】

【서류명】	특허출원서
【권리구분】	특허
【수신처】	특허청장
【참조번호】	0002
【제출일자】	2003.08.26
【국제특허분류】	H04L
【발명의 명칭】	데이터를 안정적으로 전송할 수 있는 기가비트 이더넷 기반의 수동 광가입자망 및 이를 이용한 데이터 암호화 방법
【발명의 영문명칭】	GIGABIT ETHERNET PASSIVE OPTICAL NETWORK CAPABLE OF TRANSMITTING STABILIZED DATA AND DATA ENCRYPTING METHOD USING THAT
【출원인】	
【명칭】	삼성전자 주식회사
【출원인코드】	1-1998-104271-3
【대리인】	
【성명】	이건주
【대리인코드】	9-1998-000339-8
【포괄위임등록번호】	2003-001449-1
【발명자】	
【성명의 국문표기】	이학필
【성명의 영문표기】	LEE,Hak Phil
【주민등록번호】	750128-1155218
【우편번호】	405-771
【주소】	인천광역시 남동구 만수4동 만수주공1단지아파트 103동 203호
【국적】	KR
【발명자】	
【성명의 국문표기】	박세강
【성명의 영문표기】	PARK,Se Kang
【주민등록번호】	731115-1037819
【우편번호】	463-767
【주소】	경기도 성남시 분당구 서당동 효자촌현대아파트 103동 1206호
【국적】	KR

【발명자】
【성명의 국문표기】 성환진
【성명의 영문표기】 SUNG,Whan Jin
【주민등록번호】 720605-1018018
【우편번호】 442-813
【주소】 경기도 수원시 팔달구 영통동 1020-4
【국적】 KR
【발명자】
【성명의 국문표기】 김영석
【성명의 영문표기】 KIM,Young Seok
【주민등록번호】 611021-1684623
【우편번호】 463-820
【주소】 경기도 성남시 분당구 서현동 310번지 효자촌 614동 802호
【국적】 KR
【발명자】
【성명의 국문표기】 오윤제
【성명의 영문표기】 OH,Yun Je
【주민등록번호】 620830-1052015
【우편번호】 449-915
【주소】 경기도 용인시 구성면 언남리 동일하이빌 102동 202호
【국적】 KR
【발명자】
【성명의 국문표기】 안준성
【성명의 영문표기】 AN,Jun Sung
【주민등록번호】 750718-1644043
【우편번호】 442-190
【주소】 경기도 수원시 팔달구 우만동 71-3번지 태영타운 302호
【국적】 KR
【발명자】
【성명의 국문표기】 박태성
【성명의 영문표기】 PARK,Tae Sung
【주민등록번호】 640619-1029617

【우편번호】 449-912
【주소】 경기도 용인시 구성면 마북리 삼성래미안 1차 109동 1202호
【국적】 KR

【발명자】
【성명의 국문표기】 김수형
【성명의 영문표기】 KIM,Su Hyung
【주민등록번호】 710501-1079657
【우편번호】 138-783
【주소】 서울특별시 송파구 풍납2동 우성아파트 5동 706호
【국적】 KR

【심사청구】 청구

【취지】 특허법 제42조의 규정에 의한 출원, 특허법 제60조의 규정에 의한 출원심사 를 청구합니다. 대리인
이건주 (인)

【수수료】

【기본출원료】	20 면	29,000 원
【가산출원료】	14 면	14,000 원
【우선권주장료】	0 건	0 원
【심사청구료】	12 항	493,000 원
【합계】	536,000 원	

【요약서】

【요약】

데이터를 안정적으로 전송할 수 있는 기가비트 이더넷 기반의 수동 광가입자망이 개시된다. 기가비트 이더넷 기반의 수동 광가입자망은 서비스 제공자측에 마련되고 전송매체를 통해 공개키를 수신하고 수신한 공개키로 비밀키를 암호화하여 전송하고 비밀키로 데이터를 암호화하여 전송하는 OLT(Optical Line Terminal), 및 OLT에서 상기 비밀키를 암호화하는데 이용되는 공개키를 상기 OLT로 전송하고 OLT로부터 전송된 공개키로 암호화된 비밀키를 수신하여 복호화하며 OLT로부터 전송된 비밀키로 암호화된 데이터를 수신하여 복호화된 비밀키로 복호화하는 ONT(Optical Network Terminal)를 갖는다.

【대표도】

도 3

【색인어】

OLT, ONT, PON, GE-PON, 암호화, 공개키, 비밀키

【명세서】

【발명의 명칭】

데이터를 안정적으로 전송할 수 있는 기가비트 이더넷 기반의 수동 광가입자망 및 이를 이용한 데이터 암호화 방법{GIGABIT ETHERNET PASSIVE OPTICAL NETWORK CAPABLE OF TRANSMITTING STABILIZED DATA AND DATA ENCRYPTING METHOD USING THAT}

【도면의 간단한 설명】

도 1은 기가비트 이더넷 수동 광가입자망에서 데이터의 하향 전송 구조를 나타낸 도면,

도 2는 기가비트 이더넷 수동 광가입자망에서 데이터의 상향 전송 구조를 나타낸 도면,

도 3은 본 발명에 따른 OLT와 ONT 간에 데이터를 안정적으로 송수신하기 위해 데이터를 암호화하는 GE-PON의 바람직한 실시예를 도시한 블록도,

도 4는 도 3의 OLT 키관리부 및 ONT 키관리부를 보다 상세히 나타낸 블록도,

도 5는 본 발명에 따른 GE-PON 구조에서 하나의 OLT와 다수의 ONT 간에 데이터를 안정적으로 전송할 수 있는 데이터 암호화 방법의 제1실시예를 도시한 순서도, 그리고

도 6은 본 발명에 따른 GE-PON 구조에서 하나의 OLT와 다수의 ONT 간에 데이터를 안정적으로 전송할 수 있는 데이터 암호화 방법의 제2실시예를 도시한 순서도이다.

* 도면의 주요 부분에 대한 부호의 설명 *

180 : 데이터 암호부 200 : OLT 키관리부

220 : 공개키 저장부 240 : 비밀키 암호부

260 : 비밀키 생성부 480 : 데이터 복호부

500 : ONT 키관리부 520 : 공개키 저장부

540 : 개인키 저장부 560 : 비밀키 복호부

【발명의 상세한 설명】

【발명의 목적】

【발명이 속하는 기술분야 및 그 분야의 종래기술】

<13> 본 발명은 서비스 제공자측에 마련된 하나의 OLT(Optical Line Terminal)와 사용자측에 마련된 다수의 ONT(Optical Network Terminal)로 구성된 기가비트 이더넷 기반의 수동 광가입자망(Gigabit Ethernet Passive Optical Network: GE-PON)에 관한 것으로, 보다 상세하게는, 하나의 OLT와 다수의 ONT들 간에 데이터 보안을 위한 암호화 방법에 관한 것이다.

<14> 현재에 다양한 무선망, 초고속 통신망 등등을 위시한 공공 네트웍의 확충은 온라인(online) 상에서 대량의 데이터 공유를 가능케 하고 있다. 또한, CD 및 DVD 등과 같은 저렴한 대용량 저장매체를 통한 오프라인(offline) 상에서의 데이터 공유도 매우 폭넓게 이용되고 있는 실정이다. 따라서, 사용자는 온라인 및 오프라인을 통해 공유된 수많은 종류의 데이터를 제공받을 수 있다.

<15> 이러한 온라인 및 오프라인 공유 체계는 다양하면서도 대량의 데이터를 사용자에게 용이하게 제공하고 있는데 반하여, 상업성을 띠는 여러 종류의 멀티미디어데이터 또는 보안이 필요한 데이터들에 대한 보안 체계는 매우 취약한 구조를 갖는다.

<16> 수동 광가입자망은 광케이블 망을 통해 최종사용자에게 신호를 전달하는 통신망 시스템이다. 수동 광가입자망은 통신회사에 설치되어 있는 한 대의 OLT(Optical Line Terminal)와 가입자 부근에 설치되어 있는 다수의 ONT(Optical Network Terminal)로 구성되는데, 대개 최대 32개의 ONT가 한 대의 OLT에 연결될 수 있다.

<17> 수동 광가입자망은 하나의 단독형 시스템에서, 하향으로 622 Mbps, 상향으로 155 Mbps의 대역폭을 사용자에게 제공할 수 있으며, 이 대역폭은 다수의 수동 광가입자망 사용자들에게 할당될 수 있다. 또한 수동 광가입자망은 케이블TV 시스템과 같은 대규모 시스템과 인근의 빌딩 또는 동축케이블을 이용하는 가정용 이더넷 네트웍 사이에서 트렁크로 이용될 수도 있다.

<18> 한편, OLT는 광케이블을 통해 해당 신호를 ONT에 전송한다. ONT는 OLT로부터 전송되는 신호를 수신 받아 설정된 방식에 따라 신호 처리한 후 최종 가입자에게 전송한다. 여기서, 서비스 가입자측의 전송 시스템인 ONT는 최종 사용자들에게 서비스 인터페이스를 제공하는 광통신망의 종단 장치이다.

<19> ONT는 FTTC(Fiber To The Curb), FTTB(Fiber To The Building), FTTF (Fiber To The Floor), FTTH(Fiber To The Home), 및 FTTO(Fiber To The Office) 등을 수용한다. 이에 따라, ONT는 가입자들에게 서비스 접근성이 높도록 구현한다. ONT는 가입자와 연결되어 가입자로부터 전송된 아날로그 신호를 전송하는 케이블과, OLT와 연결되어 광신호를 송수신하는 광시설들을 연결시켜주는 기능을 수행한다. 따라서, ONT는 OLT로부터 전송된 광신호를 전기신호로 변환하여 가입자에게 전송하는 광전변환 및 가입자로부터 전송된 전기신호를 광신호로 변환하여 OLT로 전송하는 전광변환을 수행한다.

<20> 도 1은 기가비트 이더넷 수동 광가입자망에서 데이터의 하향 전송 구조를 나타낸 도면이고, 도 2는 기가비트 이더넷 수동 광가입자망에서 데이터의 상향 전송 구조를 나타낸 도면이다.

<21> 도시된 바와 같이, 기가비트 이더넷 수동 광가입자망(Gigabit Ethernet Passive Optical Network System : 이하 GE-PON이라 함)은 1개의 OLT(10)가 다수의 ONT(20,22,24)와 광분배기(15)에 의해 트리(tree) 구조로 연결된 구조를 가지며, AON(Activity-on-Node) 시스템보다 저가로 효과적인 가입자망을 구성할 수 있는 방법이다.

<22> GE-PON의 형태로는 비동기 전송 모드 수동 광가입자망(Asynchronous Transfer Mode Passive Optical Network : 이하, ATM-PON이라 함)이 먼저 개발되어 표준화가 이루어졌는데, ATM-PON은 ATM의 셀(cell)을 일정한 크기로 묶은 블록(block) 형태로 상향 및 하향 전송이 이루어지게 된다. 반면, 이더넷 수동 광가입자망(E-PON)은 크기가 다른 패킷을 일정한 크기의 블록으로 묶어 전송한다. 따라서, E-PON은 ATM-PON에 비해 다소 복잡한 제어 구조를 갖는다.

<23> 도 1을 참조하여 데이터의 하향 전송에 대해 설명한다. 하향 전송(Downstream)의 경우 OLT(10)는 ONT(20,22,24)에 전송하기 위한 데이터를 브로드케스팅(broadcasting)한다. 광분배기(15)는 OLT(10)로부터 전송된 데이터가 수신되면, 각각의 ONT(20,22,24)에 수신된 데이터를 전송한다. 각각의 ONT들(20,22,24)은 광분배기(15)로부터 전송된 데이터로부터 각각의 사용자들(30,32,34)에 전송하기 위한 데이터를 검출하여 검출된 데이터만을 사용자들(30,32,34)에게 각각 전송한다.

<24> 도 2를 참조하여 데이터의 상향 전송에 대해 설명한다. 상향 전송(Upstream)의 경우 사용자들(30,32,34)로부터 전송된 각각의 데이터들은 ONT(20,22,24) 각각에 전송된다. 이때 ONT

들(20,22,24) 각각은 사용자들(30,32,34)로부터 전송된 데이터를 OLT(10)로부터 전송 허락이 약속된 조건에 따라 각각 광분배기(15)로 전송한다. 이때, 각각의 ONT들(20,22,24)은 TDM(Time Division Multiflexing) 방식으로 설정된 시간 동안 수신된 각각의 데이터를 상향 전송한다. 이에 따라, 광분배기(15)에서는 데이터의 상향 전송에 따른 데이터 충돌이 발생하지 않는다.

<25> 인터넷 기술이 발달함에 따라 서비스 가입자들은 더욱 더 많은 대역폭을 필요로하는 데이터 서비스를 요구하고 있다. 이에 따라 상대적으로 고가 장비이며 대역폭에 제한이 있고 IP 패킷을 구분(Segmentation)해야 하는 ATM(asynchronous transfer mode)기술 보다는 상대적으로 저가이며 높은 대역폭을 확보할 수 있는 기가비트 이더넷 기술을 이용한 점대 점(End-to-End) 전송을 제안하고 있다. 따라서 가입자 망의 PON 구조에서도 ATM이 아닌 이더넷 방식을 요구된다.

<26> ATM PON(Asynchronous Transfer Mode Passive Optical Network)에서 사용되고 있는 패킷 PDU(Protocol Data Unit) 암호화 방식에서는 처닝(Churning)으로 24 바이트(Bytes) 크기의 암호화 키(Key)가 사용된다. 이 방법은 1초마다 키 값이 갱신되어야 하는 암호능력을 가지고 있으며 상대적으로 간단한 알고리즘이므로 622Mbps의 속도를 가지고 있는 ATM PON에서 고속지원이 가능하도록 사용된다. 주기적으로 갱신되는 키 값들은 ONT에서 만들어져 OAM(Operations, Administration and Maintenance) 셀의 페이로드(Payload)부분에 삽입되어 각 OLT에게 전송된다.

<27> 또한, 패킷 PDU 암호화 방식으로 처닝 방식 외에 DES-CBC(Data Encryption Standard with Cipher Block Chaining) 암호화 방식을 사용하는 DOCSIS(Data Over Cable Service Interface Specification)가 있다.

<28> ATM PON의 경우, 암호화 기술의 한계와 고속 지원의 가능성으로 인하여 3 바이트(Bytes)의 처닝 키(Churning Key)를 OAM 셀에 삽입하여 사용하였으나, 이 경우 암호화 키 자체의 능력이 제한되는 한계가 있다.

<29> 기가비트 이더넷의 경우는 622Mbps의 전송속도를 갖는 ATM PON에 비해 상대적으로 고속이므로 ATM PON의 암호화 방안을 따르는 것은 기술적으로 비효율적이다. DES-CBC 암호화 방식을 사용하는 DOCSIS에서의 키 주기는 매 12시간 마다 반복되어야 악의의 사용자에 의해 감청당하는 것을 방지할 수 있다.

<30> 따라서 DES-CBC 암호화 방식을 GE-PON 에 적용할 경우 빠른 전송속도와 점-대-다점 구조에서 다수의 ONT를 관리해야하는 OLT에 비효율성을 가중시킬 수 있다. 또한 상대적으로 암호화에 취약한 점-대-다점의 구조를 가지고 있음으로 인해 상향/하향 링크의 사용자 데이터의 암호화 문제가 중요하므로 강력하고 효율적인 암호화 키 방식의 선택과 효과적인 운용이 필요하다. 그러나 현재 GE-PON의 암호화 방식 및 키 관리 스케쥴링 방안은 IEEE 802.3ah에서 표준화가 진행 중일 뿐 아직 패킷 포맷도 결정되지 않은 상태이다.

【발명이 이루고자 하는 기술적 과제】

<31> 상기와 같은 문제점을 해결하기 위한 본 발명의 목적은, 하나의 OLT와 다수의 ONT 간에 데이터를 안정적으로 송수신하기 위한 기가비트 이더넷 기반의 수동 광가입자망 및 이를 이용한 데이터 암호화 방법을 제공하는데 있다.

<32> 본 발명의 다른 목적은, 하나의 OLT에서 다수의 ONT 방향으로 하향 전송(Downstream) 시 데이터에 대한 보안을 높일 수 있는 기가비트 이더넷 기반의 수동 광가입자망 및 이를 이용한 데이터 암호화 방법을 제공하는데 있다.

【발명의 구성 및 작용】

<33> 상기와 같은 목적은 본 발명에 따라, 서비스 제공자측에 마련되고 전송매체를 통해 공개키를 수신하고 수신한 공개키로 비밀키를 암호화하여 전송하고 비밀키로 데이터를 암호화하여 전송하는 OLT(Optical Line Terminal); 및 OLT에서 상기 비밀키를 암호화하는데 이용되는 공개키를 상기 OLT로 전송하고, OLT로부터 전송된 공개키로 암호화된 비밀키를 수신하여 복호화하며, OLT로부터 전송된 비밀키로 암호화된 데이터를 수신하여 복호화된 비밀키로 복호화하는 ONT(Optical Network Terminal)를 포함하는 기가비트 이더넷 기반의 수동 광가입자망에 의해 달성된다.

<34> 바람직하게는, 상기 OLT는, GE-PON OLT MAC 모듈, GMII 모듈, OLT 키관리부, 및 데이터 암호부를 갖는다. GE-PON OLT MAC 모듈은 입력되는 데이터를 설정된 경로로 전송한다. GMII 모듈은 전송매체와 GE-PON OLT MAC 모듈 간의 인터페이스를 제공한다. OLT 키관리부는 ONT로부터 전송된 공개키 및 데이터를 암호화하기 위한 비밀키를 관리한다. 데이터 암호부는 비밀키를 이용하여 데이터를 암호화한다.

<35> 여기서 상기 GMII모듈은, PCS 모듈, PMA 모듈, 및 PMD 모듈을 갖는다. PCS 모듈은 입력되는 데이터를 설정된 블록 단위로 선택적으로 인코딩 및 디코딩하여 출력한다. PMA 모듈은 입력되는 데이터를 선택적으로 직병렬 변환하여 출력한다. PMD 모듈은 PMA모듈로부터 출력된

데이터인 전기신호를 광신호로 변환하여 전송매체로 전송하고, 전송매체로부터 수신되는 광신호를 전기신호로 변환하여 PMA 모듈로 전송한다.

<36> 상기 OLT 키관리부는, 공개키 저장부, 비밀키 생성부, 비밀키 암호부를 갖는다. 공개키 저장부는 ONT로부터 전송된 공개키를 저장한다. 비밀키 생성부는 공개키 저장부에 공개키가 저장되면, 데이터를 암호화하기 위한 비밀키를 생성한다. 비밀키 암호부는 비밀키 생성부에서 생성한 비밀키를 공개키 저장부에 저장한 공개키로 암호화한다.

<37> 상기 ONT는, GE-PON OLT MAC 모듈, GMII 모듈, ONT 키관리부, 및 데이터 복호부를 갖는다. GE-PON OLT MAC 모듈은 입력되는 데이터를 설정된 경로로 전송한다. GMII 모듈은 전송매체와 GE-PON OLT MAC 모듈 간의 인터페이스를 제공한다. ONT 키관리부는 공개키 및 개인키를 관리하고 개인키를 이용하여 OLT로부터 전송된 암호화된 비밀키를 복호한다. 데이터 복호부는 ONT 키관리부에서 복호된 비밀키를 이용하여 OLT로부터 전송된 암호화된 데이터를 복호한다. 여기서 GMII모듈은 OLT에 마련된 GMII 모듈과 동일한 구조를 갖는다.

<38> 상기 ONT 키관리부는, 공개키를 저장하는 공개키 저장부, 개인키를 저장하는 개인키 저장부, 및 개인키 저장부에 저장된 개인키를 이용하여 OLT로부터 전송된 암호화된 비밀키를 복호하여 데이터 복호부로 출력하는 비밀키 복호부를 갖는다.

<39> 본 발명에서 공개키 및 개인키는 각각 RSA 공개키 및 RSA 개인키를 의미한다. 또한, 비밀키는 AES 비밀키인다.

<40> 한편, 상기와 같은 목적은 본 발명에 따라, E-PON 구조에서 하나의 OLT와 다수의 ONT 간에 데이터를 안정적으로 송수신하기 위해 암호화 방법에 있어서, a)ONT가 공개키를 상기 OLT로 전송하는 단계; b)OLT가 ONT에서 전송한 공개키로 비밀키를 암호화하여 ONT로 전송하는 단계;

c)ONT가 OLT에서 전송한 암호화된 비밀키를 개인키를 이용하여 복호화하는 단계; d)OLT가 상기 비밀키로 데이터를 암호화하여 ONT로 전송하는 단계; e)ONT가 OLT에서 전송한 암호화된 데이터를 복호화한 비밀키를 이용하여 복호화는 단계를 포함하는 암호화 방법에 의해 달성된다.

<41> 상기 b) 단계는, ONT에서 전송한 상기 공개키를 저장하는 단계; 공개키를 저장하면 데이터를 암호화하기 위한 비밀키를 생성하는 단계; 비밀키를 공개키를 이용하여 암호화하는 단계; 및 암호화된 공개키를 ONT로 전송하는 단계를 포함한다.

<42> 본 발명에 따르면, OLT가 ONT로부터 전송된 RSA 공개키로 AES 비밀키를 암호화하여 ONT로 전송하고 AES 비밀키를 이용하여 데이터를 암호화하여 ONT로 전송함으로써, 점대 다점 구조를 갖는 GE-PON 구조에서 데이터를 효율적으로 암호화할 수 있다. 또한, ONT가 RSA 공개키를 OLT로 전송하여 공개키를 상호 공유하고 OLT가 RSA 공개키로 데이터를 암호화하는데 이용되는 AES 비밀키를 암호화하여 ONT로 전송함에 따라 비밀키를 상호 공유함으로써, 점대 다점 구조를 갖는 GE-PON 구조에서 전송하기 위한 데이터를 효율적으로 암호화할 수 있다.

<43> 이하, 본 발명의 바람직한 실시예들을 첨부한 도면을 참조하여 상세히 설명한다. 도면들 중 동일한 구성요소들은 가능한 한 어느 곳에서든지 동일한 부호들로 나타내고 있음에 유의해야 한다. 또한 본 발명의 요지를 불필요하게 흐릴 수 있는 공지 기능 및 구성에 대한 상세한 설명은 생략한다.

<44> 이하 본 발명에 따른 GE-PON 구조에서 하나의 OLT와 다수의 ONT 간에 데이터를 안정적으로 송수신하기 위해 암호화 방법에 대하여 상세히 설명한다. 본 발명에 따른 데이터 암호화는 128 비트 길이의 비밀키(Secret Key)를 사용하는 AES(Advanced Encryption Standard) 비밀키 알고리즘 또는 Rijndael 알고리즘이 이용된다. 그리고 이 비밀키를 공개된 온라인 상에서 OLT

와 ONU 간에 교환하기 위한 키 암호화는 1024 비트 길이의 공개키(Public Key) 및 개인키(Private Key)를 사용하는 RSA(Rivest, Shamir, Adleman) 공개키 알고리즘이 이용된다.

<45> AES 비밀키 알고리즘 및 RSA 공개키 알고리즘에 대한 상세한 기술은 참고문헌 R.Rivest, A.Shamir, and L.Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," Communications of the ACM, 21(2), pp. 120-126, Feb. 1978 및 참고문헌 RSA Laboratories, "PKCS #1 v2.1 : RSA Cryptography Standard," June 2002에 개시되어 있다.

<46> 전술한 바와 같이, GE-PON에서 OLT와 ONT 간의 초기 등록절차에 관한 표준은 이미 공표된 바 있으나, 데이터 송수신을 위한 데이터 암호화에 관해서는 어떤 언급도 결정된 것이 없다. 따라서 본 발명에서는 GE-PON에서 AES 비밀키 알고리즘을 이용한 데이터 암호화는 GE-PON 표준 패킷 포맷에서 주소 필드(DA(Destination Address), SA(Source Address))를 제외한 데이터 전체를 암호화한다.

<47> 또한 본 발명에서는 RSA 알고리즘을 이용하여 RSA 공개키로 AES 비밀키를 암호화하는데, 이때 암호화된 AES 비밀키는 이더넷 프레임의 사용자 데이터 PDU(Protocol Data Unit) 영역에 삽입되어 하위계층으로 전송된다.

<48> 본 발명의 다른 실시예에서는 OLT와 ONT 간에 비밀키 및 공개키 교환이 모두 이루어지기 전까지는 그 어떤 데이터도 평문(Plaintext)으로 데이터의 송수신이 없어야 하므로, OLT와 ONT 간에 표준 GE-PON 등록절차를 준수하면서 상기 등록절차 시 데이터 암호화를 위한 키 교환 절차를 포함하여 실시하고 있다.

<49> 도 3은 본 발명에 따른 OLT와 ONT 간에 데이터를 안정적으로 송수신하기 위해 데이터를 암호화하는 GE-PON의 바람직한 실시예를 도시한 블록도이다. 참고로 본 실시예의 데이터 암호

화를 위한 프로세스는 OSI(Open Systems Interconnection communications) 7계층에서 2계층에 해당하는 데이터 링크 계층(Data Link Layer) 또는 GE-PON MAC(Gigabit Ethernet Passive Optical Network Media Access Control) 계층에서 이루어진다.

<50> 도시된 바와 같이, GE-PON은 전송매체(300)를 통해 상호 채널을 설정하여 데이터를 송수신하는 OLT(100) 및 ONT(400)로 구성된다.

<51> 구체적으로 OLT(100)는 GE-PON OLT MAC모듈(120), GMII(Gigabit Media Independent Interface)모듈(130), OLT 키관리부(200), 및 데이터 암호부(180)를 갖는다.

<52> GE-PON OLT MAC모듈(120)은 OSI 7계층 중 2계층에서 입력되는 데이터에 대해서 CSMA/CD 동작을 지원한다. GMII모듈(130)은 OSI 7계층 중 1계층인 물리 계층과 2계층인 MAC 계층 사이에서 상호간에 인터페이스를 제공한다. 이것은 고속 이더넷에서 사용하고 있는 MII(Media Independent Interface)를 확장한 것으로 10Mbps, 100Mbps, 1000Mbps의 데이터 처리 속도를 지원한다. 또한 GMII모듈(130)은 독립된 8 비트의 데이터 송수신 경로를 가지고 있어서 풀 듀플렉스(full-duplex) 및 할프 듀플렉스(half-duplex)를 지원할 수 있다.

<53> GMII모듈(130)이 위치하는 GMII는 3개의 서브 계층으로 이루어진다. 즉, GMII는 PCS(Physical Coding Sublayer), PMA(Physical Medium Attachment), 및 PMD(Physical Medium Dependent)의 서브 계층으로 이루어지며, 각 서브 계층에는 이에 대응하는 각각의 모듈들이 마련된다.

<54> PCS에 마련되는 PCS모듈(140)은 입력되는 데이터를 설정된 블록 단위로 인코딩 및 디코딩한다. PMA 서브 계층에 마련되는 PMA모듈(160)은 PCS모듈(140)을 통해 PCS로부터 입력되는 데이터를 직렬로 변환하고, PMD 서브 계층으로부터 입력되는 데이터를 병렬로 변환한다. PMD

계층에 마련되는 PMD모듈(170)은 PMA모듈(160)을 통해 PMA 서브 계층으로부터 전송된 데이터인 전기신호를 광신호로 변환하여 전송매체(300)로 전송하고, 전송매체(300)로부터 수신되는 광신호를 전기신호로 변환하여 PMA 서브 계층으로 전송한다.

<55> OLT 키관리부(200)는 ONT(400)로부터 전송된 RSA 공개키를 수신하면 AES 비밀키를 생성하고, RSA 공개키를 이용하여 AES 비밀키를 암호화한다. 이렇게 암호화된 AES 비밀키는 GE-PON OLT MAC모듈(120) 및 GMII모듈(130)을 거쳐 전송매체(300)를 통해 ONT(400)로 전송된다.

<56> 데이터 암호부(180)는 상기 AES 비밀키를 이용하여 평문 데이터를 암호화한다. 이렇게 암호화된 암호문 데이터는 GE-PON OLT MAC모듈(120) 및 GMII모듈(130)을 거쳐 전송매체(300)를 통해 ONT(400)로 전송된다.

<57> 한편, ONT(400)는 GE-PON ONT MAC모듈(420), GMII모듈(430), ONT 키관리부(500), 및 데이터 복호부(480)를 갖는다.

<58> GE-PON ONT MAC모듈(420) 및 GMII모듈(430)은 OLT(100)에 마련된 GE-PON ONT MAC모듈(120) 및 GMII모듈(130)과 각각 대응하여 동일한 기능을 수행한다. ONT 키관리부(500)는 OLT(100)에서 AES 비밀키를 암호화하는데 이용되는 RSA 공개키 및 상기 RSA 공개키로 암호화된 AES 비밀키를 복호화하는데 이용되는 RSA 개인키를 구비한다.

<59> 이에 따라, ONT 키관리부(500)는 OLT(100)로부터 데이터를 서비스 받고자 하는 경우, 저장된 RSA 공개키를 GE-PON ONT MAC모듈(420) 및 GMII모듈(430)을 거쳐 전송매체(300)를 통해 OLT(100)로 전송한다. 또한, OLT(100)로 전송한 RSA 공개키로 암호화된 AES 비밀키를 수신하면, ONT 키관리부(500)는 저장된 RSA 개인키를 이용하여 암호화된 AES 비밀키를 복호화한다.

<60> 데이터 복호부(480)는 OLT(100)로부터 AES 비밀키로 암호화된 데이터를 수신하면, 수신한 암호화된 데이터를 ONT 키관리부(500)에서 복호화된 AES 비밀키를 이용하여 복호화한다.

<61> 따라서, OLT(100)가 ONT(400)로부터 전송된 RSA 공개키로 AES 비밀키를 암호화하여 ONT(400)로 전송하고 AES 비밀키를 이용하여 데이터를 암호화하여 ONT(400)로 전송함으로써, 점대 다점 구조를 갖는 GE-PON 구조에서 데이터를 효율적으로 암호화할 수 있다.

<62> 또한, ONT(400)가 RSA 공개키를 OLT(100)로 전송하여 공개키를 상호 공유하고 OLT(100)가 RSA 공개키로 데이터를 암호화하는데 이용되는 AES 비밀키를 암호화하여 ONT(400)로 전송함에 따라 비밀키를 상호 공유함으로써, 점대 다점 구조를 갖는 GE-PON 구조에서 전송하기 위한 데이터를 효율적으로 암호화할 수 있다.

<63> 도 4는 도 3의 OLT 키관리부(200) 및 ONT 키관리부(500)를 보다 상세히 나타낸 블록도이다.

<64> OLT 키관리부(200)는 공개키 저장부(220), 비밀키 암호부(240), 및 비밀키 생성부(260)를 갖는다. 공개키 저장부(220)는 ONT(400)에서 전송된 RSA 공개키를 저장한다. 비밀키 암호부(240)는 공개키 저장부(220)에 저장된 RSA 공개키를 이용하여 AES 비밀키를 암호화한다. 비밀키 생성부(260)는 OLT(100)에서 RSA 공개키를 수신하면 AES 비밀키를 생성하여 비밀키 암호부(240)에 제공한다. 이에 따라, 비밀키 암호부(240)는 공개키 저장부(220)에 저장한 RSA 공개키를 이용하여 비밀키 생성부(260)에서 생성한 AES 비밀키를 암호화하여 GE-PON OLT MAC(120)로 전송한다.

<65> 한편 데이터 암호부(180)는 비밀키 생성부(260)에서 생성한 AES 비밀키를 이용하여 입력되는 데이터를 암호화하고, 암호화된 데이터를 GE-PON OLT MAC(120)로 전송한다.

<66> ONT 키관리부(500)는 공개키 저장부(520), 개인키 저장부(540), 및 비밀키 복호부(560)를 갖는다.

<67> 공개키 저장부(520)는 OLT(100)에서 AES 비밀키를 암호화하는데 이용되는 RSA 공개키를 저장한다. OLT(100)로부터 데이터를 서비스 받고자 하는 경우, ONT 키관리부(500)는 공개키 저장부(520)에 저장된 RSA 공개키를 GE-PON OLT MAC(420)로 전송한다. 개인키 저장부(540)는 OLT(100)로부터 전송된 RSA 공개키로 암호화된 AES 암호키를 복호화하는데 이용되는 RSA 개인키를 저장한다. 비밀키 복호부(560)는 OLT(100)로부터 암호화된 AES 비밀키를 수신하면, 개인키 저장부(540)에 저장된 RSA 개인키를 이용하여 암호화된 AES 비밀키를 복호화한다.

<68> 한편 데이터 복호부(480)는 OLT(100)로부터 암호화된 데이터를 수신하면, 비밀키 복호부(560)에서 복호된 AES 비밀키를 이용하여 암호화된 데이터를 복호화한다.

<69> 따라서, OLT(100) 및 ONT(400)가 RSA 공개키 및 AES 비밀키를 상호 공유하고 데이터를 AES 비밀키로 암호화하여 ONT(400)로 전송함으로써, 보다 안정된 보안성을 갖는 데이터의 전송이 가능하다.

<70> 도 5는 본 발명에 따른 GE-PON 구조에서 하나의 OLT와 다수의 ONT 간에 데이터를 안정적으로 전송할 수 있는 데이터 암호화 방법의 제1실시예를 도시한 순서도이다.

<71> 먼저, ONT(400)는 OLT(100)로부터 서비스를 제공받고자 하는 경우, 등록을 요구하는 신호 및 공개키 저장부(520)에 저장된 RSA 공개키를 OLT(100)로 전송한다(S100). OLT(100)는 ONT(400)로부터 전송된 등록요구신호를 수신하면 수신한 RSA 공개키를 공개키 저장부(220)에 등록 및 저장한다(S110).

<72> 이때, 비밀키 생성부(260)는 RSA 공개키가 공개키 저장부(220)에 등록 및 저장되면, AES 비밀키를 생성하여 비밀키 암호부(240)에 제공한다(S120). 비밀키 암호부(240)는 공개키 저장부(240)에 저장된 RSA 공개키를 이용하여 비밀키 생성부(260)에서 제공한 AES 비밀키를 암호화한다(S130). OLT(100)는 비밀키 암호부(240)에서 암호화된 AES 암호키를 ONT(400)로 전송한다(S140).

<73> ONT(400)의 비밀키 복호부(560)는 OLT(100)로부터 전송된 암호화된 AES 비밀키를 개인키 저장부(540)에 저장된 RSA 개인키를 이용하여 복호화하고 복호화된 AES 비밀키를 저장한다(S150). ONT(400)는 AES 비밀키에 대한 복호화가 완료되면, 복호화 완료정보를 OLT(100)로 전송한다(S160). OLT(100)가 복호화 완료정보를 수신하면, OLT(100)는 해당 데이터를 비밀키 생성부(260)에서 생성한 AES 암호키를 이요하여 암호화하여 ONT(400)로 전송하고 이에 대해 ONT(400)가 응답하는 데이터 전송을 수행한다(S170).

<74> 따라서, RSA 공개키와 AES 비밀키를 OLT(100)와 ONT(400)가 상호 공유하고 AES 비밀키를 이용하여 데이터를 암호화하여 ONT(400)로 전송함으로써, 점대 다점 구조를 갖는 GE-PON 구조에서 데이터를 효율적으로 암호화할 수 있다.

<75> 도 6은 본 발명에 따른 GE-PON 구조에서 하나의 OLT와 다수의 ONT 간에 데이터를 안정적으로 전송할 수 있는 데이터 암호화 방법의 제2실시예를 도시한 순서도이다. 본 실시예는 OLT(100)와 ONT(400) 간의 초기 등록 단계에서 데이터 암호화 방법을 적용한 것이다. 도면에서 ONT1(400a) 및 ONT2(400b)의 내부 구성은 도 3 및 도 4에 도시된 ONT(400)와 동일한 구성을 갖는다.

<76> 본 실시예에 따른 데이터의 암호화 방법은 크게 초기 탐색단계(S200), 공개키전송 및 LLID(Logical Link ID)할당단계(S300), 비밀키 전송 및 시간할당단계(S400), 키공유상태확인

및 대역폭할당단계(S500), 및 통신수행단계(S600)로 수행된다. 이를 보다 상세히 살펴보면 아래와 같다.

<77> OLT(100)는 최초 전원이 입력되어 구동되면, 통신 매체를 통해 연결되어 있는 ONT들을 탐색하기 위해 게이트신호를 각각의 ONT들에게 전송한다(S220a,S220b). 본 실시예에서는 다수의 ONT들 중 ONT1(400a) 및 ONT2(400b)를 예로 설명한다.

<78> OLT(100)는 등록을 요구하는 신호가 수신될 때까지 소정 시간 간격으로 ONT1(400a) 및 ONT2(400b)에게 게이트신호를 전송한다(S320a,S320b). ONT1(400a) 및 ONT2(400b)는 OLT(100)로부터 전송된 게이트신호를 수신하면, 각각에 대하여 등록을 요구하는 신호(등록요구신호) 및 각 공개키 저장부에 저장된 각각의 RSA 공개키를 OLT(100)로 전송한다(S340,S350).

<79> OLT(100)는 ONT1(400a) 및 ONT2(400b)로부터 전송된 각 등록요구신호 및 RSA 공개키를 수신하면, ONT1(400a) 및 ONT2(400b)를 등록하고 각 RSA 공개키를 공개키 저장부(220)에 등록 및 저장하며 ONT1(400a) 및 ONT2(400b)에 대하여 LLID를 부여한다. 여기서 OLT(100)는 ONT1(400a) 및 ONT2(400b)의 등록정보 및 LLID할당정보를 ONT1(400a) 및 ONT2(400b)에 대응되게 전송한다(S360,S370).

<80> 한편, OLT(100)는 ONT1(400a) 및 ONT2(400b)로부터 전송된 각 RSA 공개키를 이용하여 AES 비밀키를 생성하고 암호화하는 동작을 수행하는데, 이러한 과정을 수행하는데 소정의 시간이 필요하다. 따라서, 이러한 과정을 수행하는 동안 OLT(100)는 RSA 공개키를 이용하여 AES 비밀키를 암호화가 진행중이라는 정보(암호화 진행정보(Null))를 ONT1(400a) 및 ONT2(400b)에 각각 전송한다(S420,S430). 각 ONT1(400a) 및 ONT2(400b)는 암호화 진행정보를 수신하고 이에 대한 응답정보(널(Null) 응답정보)를 OLT(100)로 전송한다(S440,S450).

<81> 이러한 과정을 수행하는 중에 RSA 공개키를 이용하여 AES 비밀키를 암호화가 완료되면, OLT(100)는 암호화된 AES 비밀키를 대응하는 ONT1(400a) 및 ONT2(400b)에 전송한다(S460,S470). OLT(100)로부터 암호화된 AES 비밀키를 수신한 ONT1(400a) 및 ONT2(400b)는 암호화된 AES 비밀키를 RSA 개인키를 이용하여 복호화하고 이에 대한 복호 및 응답정보를 OLT(100)로 전송한다(S480,S490).

<82> OLT(100)는 ONT1(400a) 및 ONT2(400b)로부터 복호 및 응답정보를 수신하면, 전송허락정보를 ONT1(400a) 및 ONT2(400b)에 전송한다(S520,S530). 여기서 전송허락정보에는 각 ONT1(400a) 및 ONT2(400b)에 대한 대역폭 할당정보 및 RSA 공개키 및 AES 비밀키에 대한 공유 상태 정보가 포함된다. ONT1(400a) 및 ONT2(400b)는 전송허락정보를 수신하고 이에 대한 응답정보를 OLT(100)로 전송한다(S540,S550).

<83> 전술한 과정을 통해 RSA 공개키 및 AES 비밀키를 상호 공유한 OLT(100) 및 ONT1(400a), ONT2(400b)는 AES 비밀키를 이용하여 암호화된 데이터를 상호 전송한다(S560,S570).

<84> 따라서, GE-PON에서 OLT(100)와 다수의 ONT들이 RSA 공개키 및 AES 비밀키를 상호 일대일로 대응하여 공유하고 해당 AES 비밀키를 이용하여 데이터를 암호화하여 ONT들로 전송하더라도 이를 복호할 수 있는 해당 AES 비밀키를 구비하고 있는 ONT만이 해당 AES 비밀키를 이용하여 데이터를 복호할 수 있기 때문에, 점대 다점 구조를 갖는 네트워크 구조에서 데이터를 효율적으로 암호화할 수 있다.

【발명의 효과】

<85> 본 발명에 따르면, OLT가 ONT로부터 전송된 RSA 공개키로 AES 비밀키를 암호화하여 ONT로 전송하고 AES 비밀키를 이용하여 데이터를 암호화하여 ONT로 전송함으로써, 점대 다점 구조를 갖는 GE-PON 구조에서 데이터를 효율적으로 암호화할 수 있다.

<86> 또한, ONT가 RSA 공개키를 OLT로 전송하여 공개키를 상호 공유하고 OLT가 RSA 공개키로 데이터를 암호화하는데 이용되는 AES 비밀키를 암호화하여 ONT로 전송함에 따라 비밀키를 상호 공유함으로써, 점대 다점 구조를 갖는 GE-PON 구조에서 전송하기 위한 데이터를 효율적으로 암호화할 수 있다.

<87> 더구나, GE-PON에서 OLT와 다수의 ONT들이 RSA 공개키 및 AES 비밀키를 상호 일대일로 대응하여 공유하고 해당 AES 비밀키를 이용하여 데이터를 암호화하여 ONT들로 전송하더라도 이를 복호할 수 있는 해당 AES 비밀키를 구비하고 있는 ONT만이 해당 AES 비밀키를 이용하여 데이터를 복호화함으로써, 점대 다점 구조를 갖는 네트워크 구조에서 데이터를 효율적으로 암호화할 수 있다.

<88> 이상에서는 본 발명에서 특정의 바람직한 실시예에 대하여 도시하고 또한 설명하였다. 그러나, 본 발명은 상술한 실시예에 한정되지 아니하며, 특허 청구의 범위에서 첨부하는 본 발명의 요지를 벗어남이 없이 당해 발명이 속하는 기술분야에서 통상의 지식을 가진 자라면 누구든지 다양한 변형 실시가 가능할 것이다.

【특허청구범위】

【청구항 1】

기가비트 이더넷 기반의 수동 광가입자망에 있어서,

서비스 제공자측에 마련되고 전송매체를 통해 공개키를 수신하고 상기 수신한 공개키로 비밀키를 암호화하여 전송하고 상기 비밀키로 데이터를 암호화하여 전송하는 OLT(Optical Line Terminal); 및

상기 OLT에서 상기 비밀키를 암호화하는데 이용되는 상기 공개키를 상기 OLT로 전송하고, 상기 OLT로부터 전송된 상기 공개키로 암호화된 비밀키를 수신하여 복호화하며, 상기 OLT로부터 전송된 상기 비밀키로 암호화된 데이터를 수신하여 상기 복호화된 비밀키로 복호화하는 ONT(Optical Network Terminal)를 포함하는 것을 특징으로 하는 기가비트 이더넷 기반의 수동 광가입자망.

【청구항 2】

제 1항에 있어서,

상기 OLT는,

입력되는 데이터를 설정된 경로로 전송하는 GE-PON OLT MAC 모듈;

전송매체와 상기 GE-PON OLT MAC 모듈 간의 인터페이스를 제공하는 GMII 모듈;

상기 ONT로부터 전송된 공개키 및 상기 데이터를 암호화하기 위한 비밀키를 관리하는 OLT 키관리부; 및

상기 비밀키를 이용하여 상기 데이터를 암호화하는 데이터 암호부를 포함하는 것을 특징으로 하는 기가비트 이더넷 기반의 수동 광가입자망.

【청구항 3】

제 2항에 있어서,

상기 GMII모듈은,

입력되는 데이터를 설정된 블록 단위로 선택적으로 인코딩 및 디코딩하여 출력하는 PCS 모듈;

입력되는 데이터를 선택적으로 직병렬 변환하여 출력하는 PMA 모듈; 및

PMA모듈로부터 출력된 데이터인 전기신호를 광신호로 변환하여 상기 전송매체로 전송하고, 상기 전송매체로부터 수신되는 광신호를 전기신호로 변환하여 상기 PMA 모듈로 전송하는 PMD 모듈을 포함하는 것을 특징으로 하는 기가비트 이더넷 기반의 수동 광가입자망.

【청구항 4】

제 2항에 있어서,

상기 OLT 키관리부는,

상기 ONT로부터 전송된 공개키를 저장하는 공개키 저장부;

상기 공개키 저장부에 상기 공개키가 저장되면, 상기 데이터를 암호화하기 위한 비밀키를 생성하는 비밀키 생성부; 및

상기 비밀키 생성부에서 생성한 비밀키를 상기 공개키 저장부에 저장한 공개키로 암호화하는 비밀키 암호부를 포함하는 것을 특징으로 하는 기가비트 이더넷 기반의 수동 광가입자망.

【청구항 5】

제 1항에 있어서,

상기 ONT는,

입력되는 데이터를 설정된 경로로 전송하는 GE-PON OLT MAC 모듈;

전송매체와 상기 GE-PON OLT MAC 모듈 간의 인터페이스를 제공하는 GMII 모듈;

상기 공개키 및 개인키를 관리하고 상기 개인키를 이용하여 상기 OLT로부터 전송된 암호화된 비밀키를 복호하는 ONT 키관리부; 및

상기 ONT 키관리부에서 복호된 비밀키를 이용하여 상기 OLT로부터 전송된 암호화된 데이터를 복호하는 데이터 복호부를 포함하는 것을 특징으로 하는 기가비트 이더넷 기반의 수동 광가입자망.

【청구항 6】

제 5항에 있어서,

상기 GMII모듈은,

입력되는 데이터를 설정된 블록 단위로 선택적으로 인코딩 및 디코딩하여 출력하는 PCS 모듈;

입력되는 데이터를 선택적으로 직병렬 변환하여 출력하는 PMA 모듈; 및

PMA모듈로부터 출력된 데이터인 전기신호를 광신호로 변환하여 상기 전송매체로 전송하고, 상기 전송매체로부터 수신되는 광신호를 전기신호로 변환하여 상기 PMA 모듈로 전송하는 PMD 모듈을 포함하는 것을 특징으로 하는 기가비트 이더넷 기반의 수동 광가입자망.

【청구항 7】

제 5항에 있어서,

상기 ONT 키관리부는,

상기 공개키를 저장하는 공개키 저장부;

상기 개인키를 저장하는 개인키 저장부; 및

상기 개인키 저장부에 저장된 개인키를 이용하여 상기 OLT로부터 전송된 암호화된 비밀키를 복호하여 상기 데이터 복호부로 출력하는 비밀키 복호부를 포함하는 것을 특징으로 하는 기가비트 이더넷 기반의 수동 광가입자망.

【청구항 8】

제 1항에 있어서,

상기 공개키 및 상기 개인키는 각각 RSA 공개키 및 RSA 개인키인 것을 특징으로 하는 기가비트 이더넷 기반의 수동 광가입자망.

【청구항 9】

제 1항에 있어서,

상기 비밀키는 AES 비밀키인 것을 특징으로 하는 기가비트 이더넷 기반의 수동 광가입자망.

【청구항 10】

E-PON 구조에서 하나의 OLT와 다수의 ONT 간에 데이터를 안정적으로 송수신하기 위해 암호화 방법에 있어서,

a) 상기 ONT가 공개키를 상기 OLT로 전송하는 단계;

b)상기 OLT가 상기 ONT에서 전송한 공개키로 비밀키를 암호화하여 상기 ONT로 전송하는 단계;

c) 상기 ONT가 상기 OLT에서 전송한 암호화된 비밀키를 개인키를 이용하여 복호화하는 단계;

d)상기 OLT가 상기 비밀키로 데이터를 암호화하여 상기 ONT로 전송하는 단계;

e)상기 ONT가 상기 OLT에서 전송한 암호화된 데이터를 상기 복호화한 비밀키를 이용하여 복호화는 단계를 포함하는 것을 특징으로 하는 암호화 방법.

【청구항 11】

제 10항에 있어서,

상기 b) 단계는,

상기 ONT에서 전송한 상기 공개키를 저장하는 단계;

상기 공개키를 저장하면 상기 데이터를 암호화하기 위한 비밀키를 생성하는 단계;

상기 비밀키를 상기 공개키를 이용하여 암호화하는 단계; 및

상기 암호화된 공개키를 상기 ONT로 전송하는 단계를 포함하는 것을 특징으로 하는 암호화 방법.

【청구항 12】

E-PON 구조에서 하나의 OLT와 다수의 ONT 간에 데이터를 안정적으로 송수신하기 위해 암호화 방법에 있어서,

상기 OLT가 전원이 입력되어 구동되면, 전송매체를 통해 연결된 ONT를 탐색하기 위한 게이트신호를 상기 ONT로 전송하는 단계;

상기 ONT가 상기 게이트신호에 대응하는 등록요구신호 및 공개키를 상기 OLT로 전송하는 단계;

상기 OLT가 상기 ONT에서 전송한 등록요구신호에 대응하여 상기 ONT를 등록하고, 상기 ONT에 대하여 LLID를 부여하여 이에 대한 정보를 상기 ONT로 전송하는 단계;

상기 OLT가 상기 공개키로 비밀키를 암호화하여 상기 ONT로 전송하는 단계;

상기 ONT가 상기 OLT에서 전송한 암호화된 비밀키를 개인키를 이용하여 복호화하는 단계;

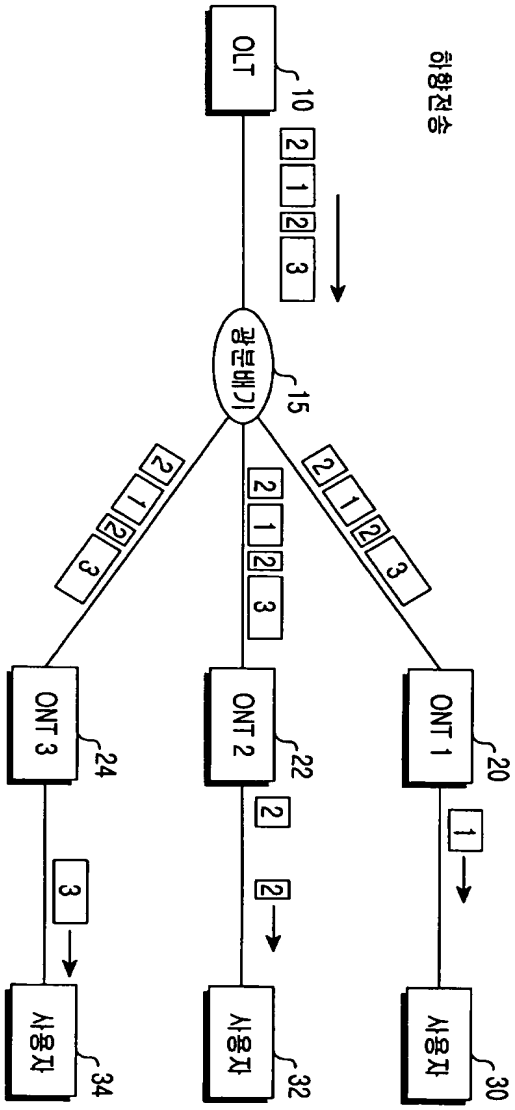
상기 OLT 및 상기 ONT가 상호 상기 공개키 및 상기 비밀키의 공유를 확인하고 상기 OLT가 상기 ONT에 데이터 전송에 필요한 대역폭을 할당하는 단계;

상기 OLT가 상기 비밀키로 데이터를 암호화하여 상기 ONT로 전송하는 단계; 및

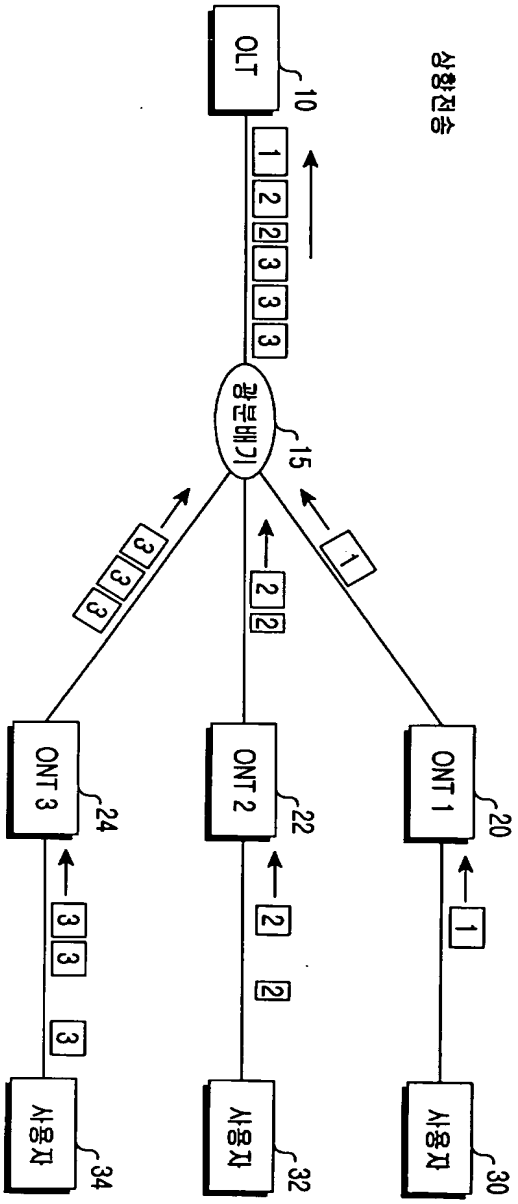
상기 ONT가 상기 OLT에서 전송한 암호화된 데이터를 상기 복호화한 비밀키를 이용하여 복호화는 단계를 포함하는 것을 특징으로 하는 암호화 방법.

【도면】

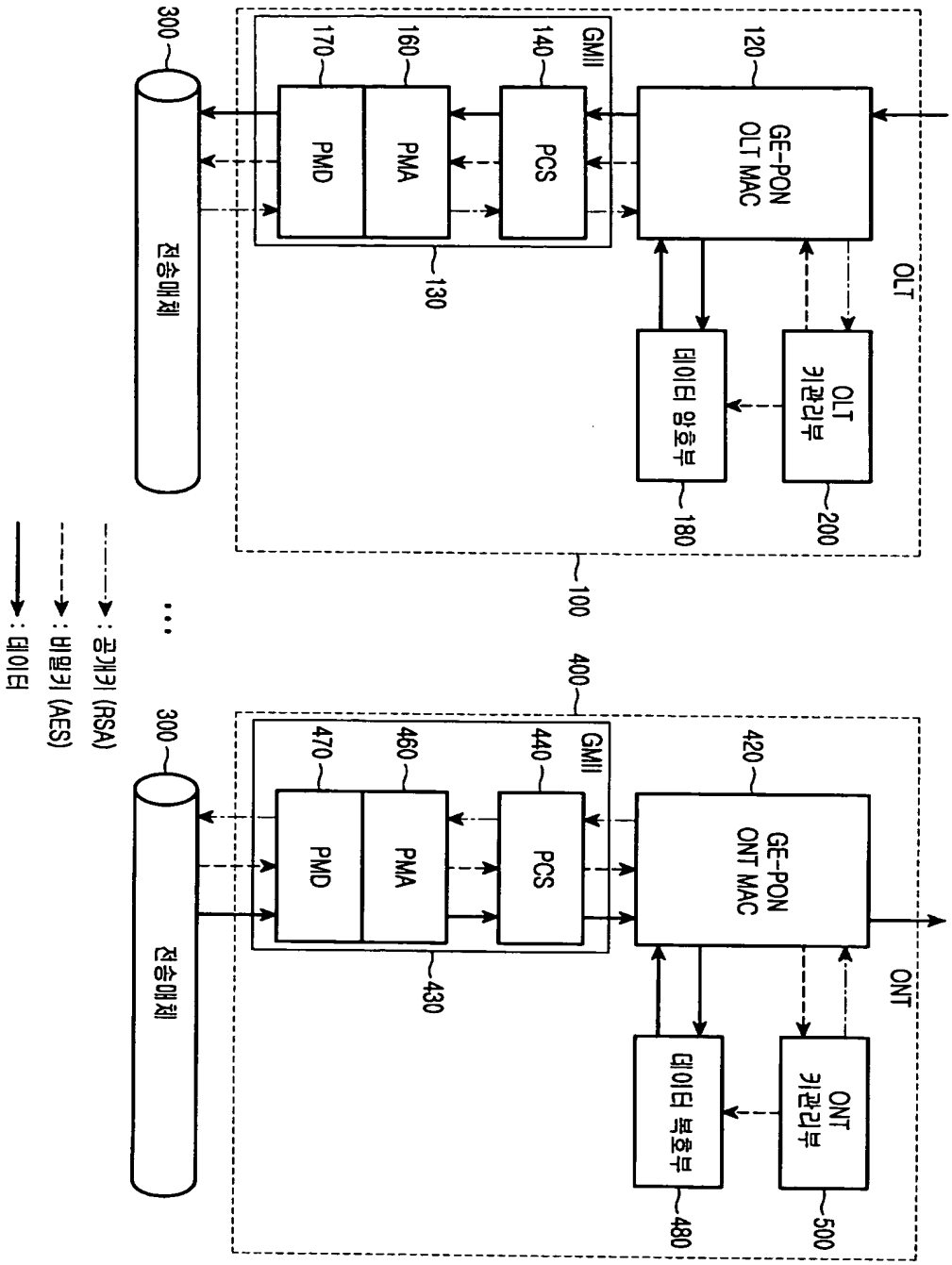
【도 1】



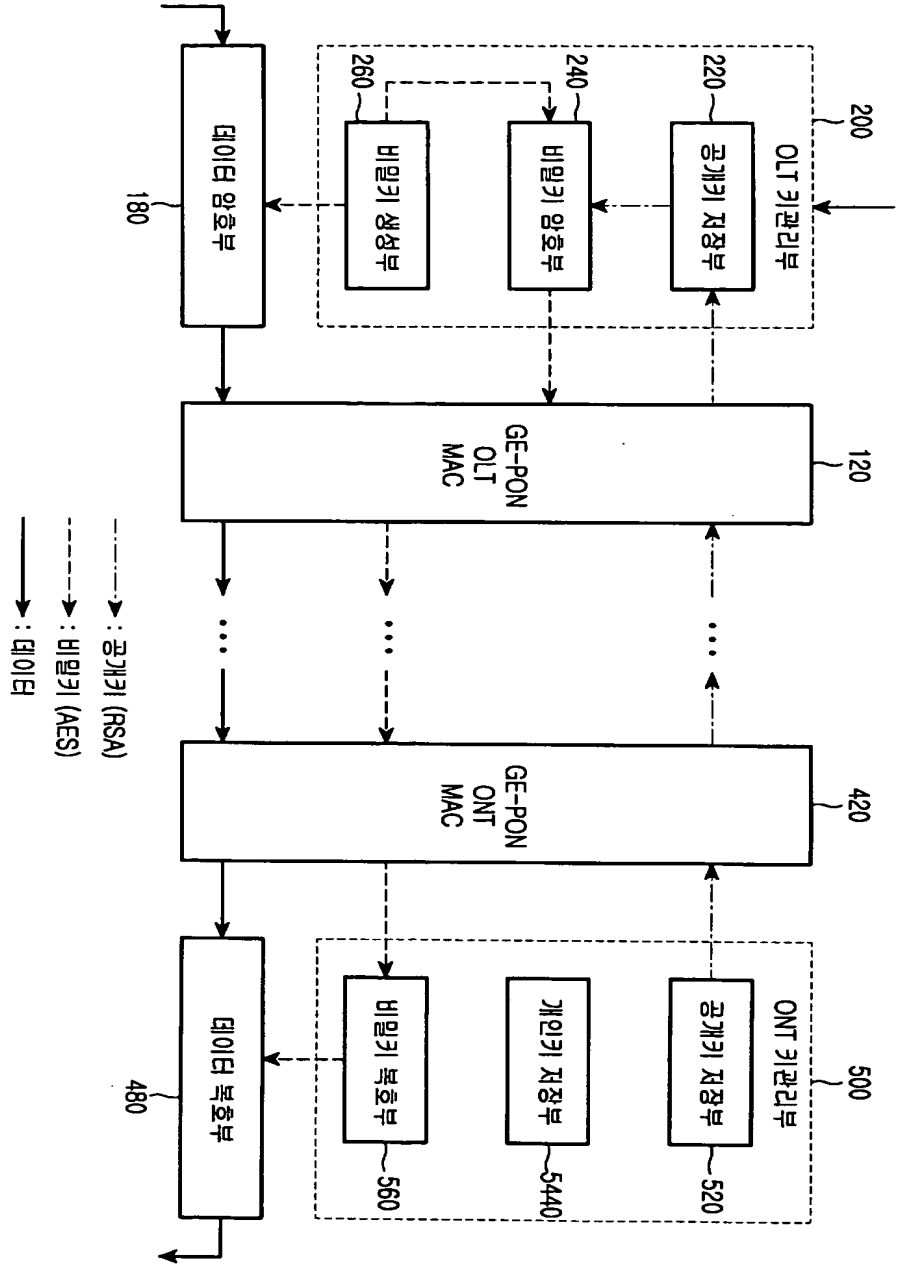
【도 2】


OLT
10
상향전송
1 2 2 3 3 3
광분배기
15
3 3 3
2 2
1
ONT 3
24
ONT 2
22
ONT 1
20
3 3 3
2 2
1
사용자
34
사용자
32
사용자
30

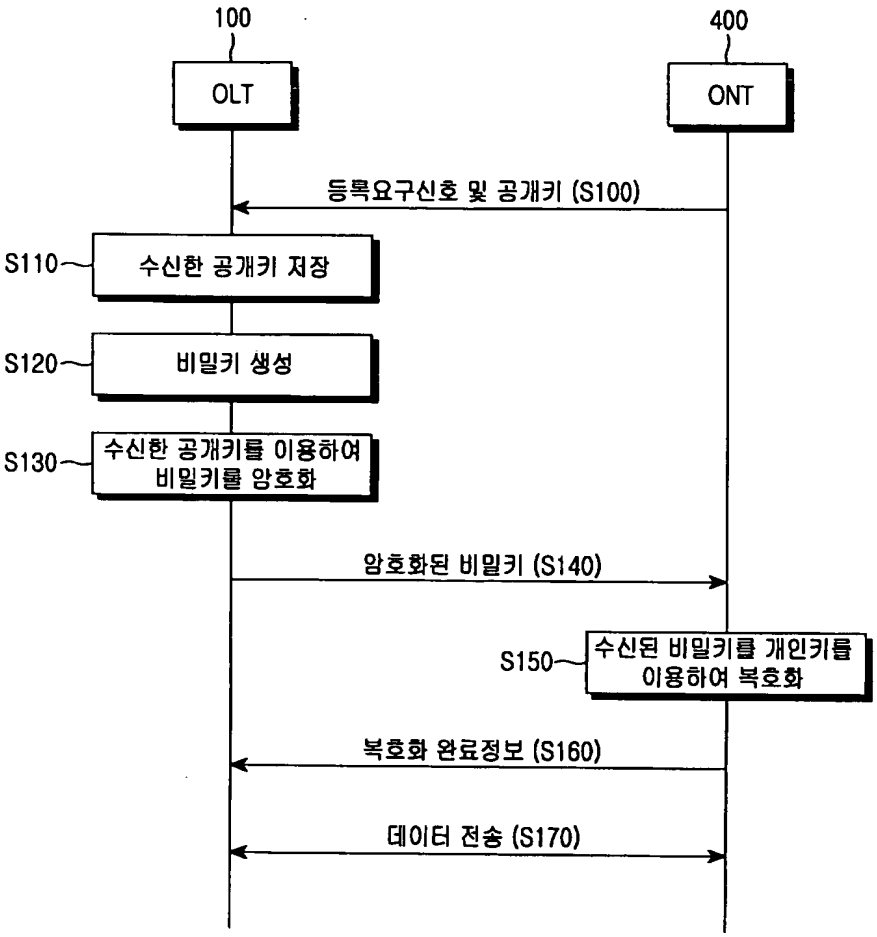
【도 3】


300
170
160
140
GMII
120
PMD
PMA
PCS
GE-PON
OLT MAC
전송매체
130
OLT
데이터 암호부
OLT
키관리부
180
200
100
400
300
470
460
440
420
PMD
PMA
PCS
GE-PON
ONT MAC
전송매체
430
ONT
데이터 복호부
ONT
키관리부
480
500
: 공개키 (RSA)
: 비밀키 (AES)
: 데이터

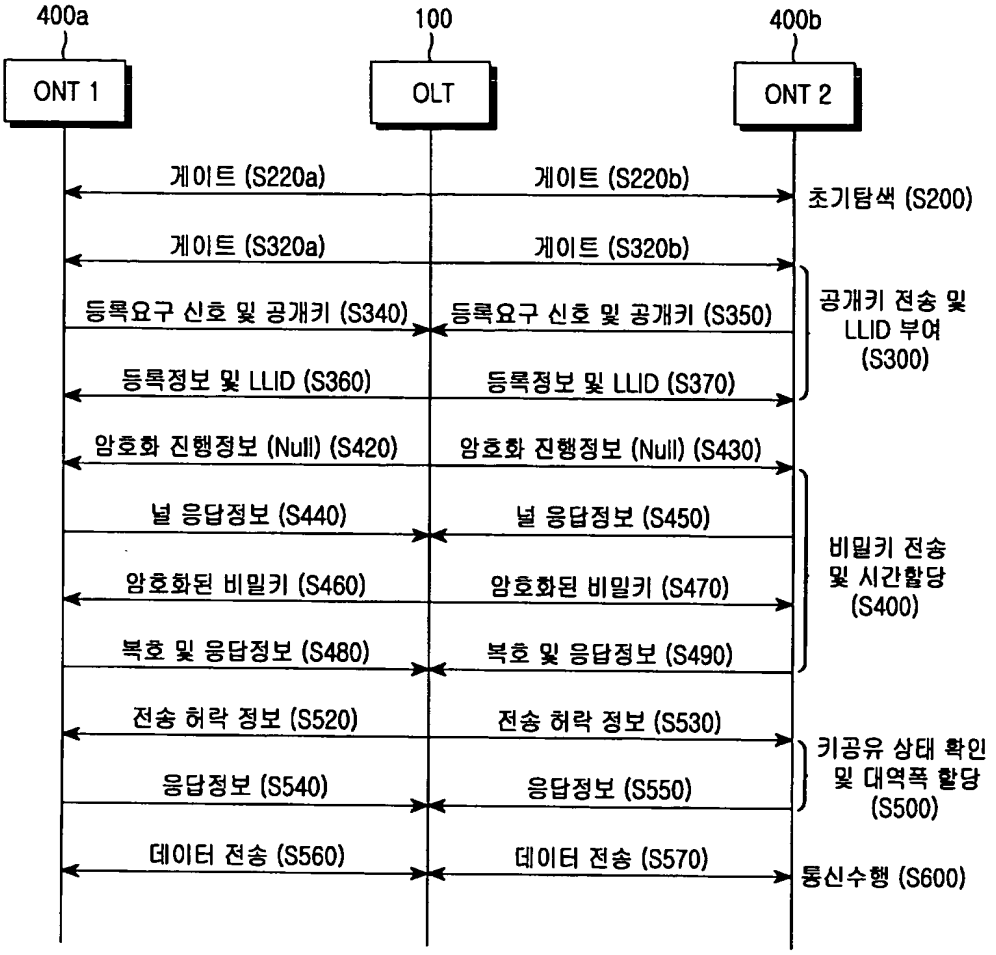
【도 4】


데이터 암호부
180
비밀키 생성부
260
비밀키 암호부
240
공개키 저장부
220
OLT 키관리부
200
GE-PON OLT MAC
120
GE-PON ONT MAC
420
데이터 복호부
480
비밀키 복호부
560
개인키 저장부
540
공개키 저장부
520
ONT 키관리부
500
: 공개키 (RSA)
: 비밀키 (AES)
: 데이터

【도 5】


100
400
OLT
ONT
등록요구신호 및 공개키 (S100)
S110
수신한 공개키 저장
S120
비밀키 생성
S130
수신한 공개키를 이용하여 비밀키를 암호화
암호화된 비밀키 (S140)
S150
수신된 비밀키를 개인키를 이용하여 복호화
복호화 완료정보 (S160)
데이터 전송 (S170)

【도 6】


400a
100
400b
ONT 1
OLT
ONT 2
게이트 (S220a)
게이트 (S220b)
초기탐색 (S200)
게이트 (S320a)
게이트 (S320b)
등록요구 신호 및 공개키 (S340)
등록요구 신호 및 공개키 (S350)
공개키 전송 및 LLID 부여 (S300)
등록정보 및 LLID (S360)
등록정보 및 LLID (S370)
암호화 진행정보 (Null) (S420)
암호화 진행정보 (Null) (S430)
널 응답정보 (S440)
널 응답정보 (S450)
암호화된 비밀키 (S460)
암호화된 비밀키 (S470)
비밀키 전송 및 시간할당 (S400)
복호 및 응답정보 (S480)
복호 및 응답정보 (S490)
전송 허락 정보 (S520)
전송 허락 정보 (S530)
응답정보 (S540)
응답정보 (S550)
키공유 상태 확인 및 대역폭 할당 (S500)
데이터 전송 (S560)
데이터 전송 (S570)
통신수행 (S600)